View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by UC Hastings Scholarship Repository (University of California, Hastings College of the Law)

Hastings Communications and Entertainment Law Journal

Volume 38 | Number 1 Article 5

1-1-2015

A Call for Minority Involvement in Cybersecurity Legislation Reform and Civil Rights Protests: Lessons from the Anti-SOPA/PIPA Demonstrations.

Kiran Sidhu

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

Part of the Communications Law Commons, Entertainment, Arts, and Sports Law Commons, and the Intellectual Property Law Commons

Recommended Citation

Kiran Sidhu, *A Call for Minority Involvement in Cybersecurity Legislation Reform and Civil Rights Protests: Lessons from the Anti-SOPA/PIPA Demonstrations.*, 38 Hastings Comm. & Ent. L.J. 117 (2015).
Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol38/iss1/5

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Communications and Entertainment Law Journal by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.

A Call for Minority Involvement in Cybersecurity Legislation Reform and Civil Rights Protests: Lessons from the Anti-SOPA/PIPA Demonstrations.

by KIRAN SIDHU[*]

[*] J.D. Candidate 2016, University of California, Hastings College of the Law.

> "[O]ur task is not to fashion legislation which seems adequate for the present period of national calm and recent revelations of intelligence abuses. We do not need to draft safeguards for an Attorney General who makes clear . . . his determination to prevent abuse. We must legislate for the next periods of social turmoil and passionate dissent, when the current outrage has faded and those in power may again be tempted to investigate their critics in the name of national security."[1]

–Chairman Frank Church, Final [Senate] Report of the Select Committee to Study Governmental Operations With Respect to Intelligence Activities.

I. Introduction: Remembering "Bloody Sunday" and COINTELPRO Surveillance and Its Connection to the Black Lives Matter Movement

March 7, 2015, marked the fiftieth anniversary of "Bloody Sunday," a day in civil rights history wherein Reverend Hosea Williams and John Lewis led a voting rights march with about 650 peaceful demonstrators from Selma, Alabama, toward the state's capital in Montgomery.[2] Six blocks in, as they attempted to cross over the Edmund Pettus Bridge, Governor George Wallace dispatched the sheriff's deputies and state troopers, who violently attacked the demonstrators with clubs and tear gas, severely injuring many of them.[3] The violence did not deter the demonstrators.

Ten days later, in *Williams v. Wallace*,[4] Federal District Court Judge Frank M. Johnson, Jr. ruled that plaintiff demonstrators' proposed plan to peacefully march along U.S. Highway 80 from Selma to Montgomery was a reasonable "exercise of a constitutional right of assembly and free movement within the State of Alabama for the purpose of petitioning their State government for the redress of their grievances."[5] Judge Johnson found that particularly in Selma, the evidence showed "an almost continuous pattern of . . . harassment, intimidation, coercion, threatening

1. SENATE SELECT COMM. TO STUDY GOV'T OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, bk. III, at 362 (2d Sess. 1976) [hereinafter SENATE SELECT COMM.], http://www.intelligence.senate.gov/sites/default/files/94755_III.pdf.

2. *Commemorating the 1965 Selma to Montgomery March*, THE DREAM MARCHES ON http://dreammarcheson.com/ (last visited Mar. 6, 2015).

3. *Id.*

4. 240 F. Supp. 100, 108 (M.D. Ala. 1965).

5. *Id.*

conduct, and sometimes, brutal mistreatment" of Black[6] citizens attempting to register to vote.[7] Judge Johnson held that the wrongs and injustice inflicted upon the demonstrators, and members of their class had "clearly exceeded . . . the outer limits of what is constitutionally permissible,"[8] and as such, he issued an injunction enjoining Governor Wallace and the Sheriff James Gardner "Jim" Clark, Jr. from intimidating, threatening, coercing or interfering with the march.[9] On March 21, about 3,200 marchers set out for Montgomery. By the time they reached Montgomery four days later, they were 25,000-strong.[10] Less than five months afterwards, President Lyndon Johnson signed the Voting Rights Act of 1965.[11]

While African Americans[12] saw some legislative and jurisprudential victories as a result of this wave of protest activity in the 1950s and 1960s, their "subversive" behavior also drew the attention of the Federal Bureau of Intelligence ("FBI"). As a result, this period also marked the beginning of government surveillance programs, most famously the FBI's Counter Intelligence Program ("COINTELPRO"),[13] which targeted Black Americans demonstrating and organizing against segregation and structural racism.[14] COINTELPRO marked the first known "systemic attempt to infiltrate, spy on, and disrupt activists in the name of national security."[15]

Then-*Washington Post* reporter William Greider wrote that the COINELPRO surveillance files offered "the public and Congress an

6. This note will capitalize the word Black to refer to people of the African Diaspora. *See* Lori L. Tharpes, *The Case for Black with a Capital B*, N.Y. TIMES (Nov. 18, 2014), http://www.nytimes.com/2014/11/19/opinion/the-case-for-black-with-a-capital-b.html?smid=tw-share&_r=2 ("When speaking of a culture, ethnicity or group of people, the name should be capitalized. Black with a capital B refers to people of the African diaspora. Lowercase black is simply a color.").

7. *Williams*, 240 F. Supp. at 104.

8. *Id.* at 108.

9. *Id.* at 109.

10. *Selma-to-Montgomery March*, NAT'L PARK SERV., U.S. DEP'T OF THE INTERIOR, http://www.nps.gov/nr/travel/civilrights/al4.htm (last visited Mar. 3, 2015).

11. *Id.*

12. This note uses the terms African American and Black interchangeably. From my experience, a greater number of people identify with the terms Black and White than African American and European American or Caucasian when discussing race. This is, in large part, due to the fact that Black is a term that does not only describe African Americans, but also Black Caribbeans, Africans, Afro-Latinos, people of African descent, and biracial individuals.

13. *COINTELPRO*, *FBI Records: The Vault*, FED. BUREAU OF INVESTIGATION, http://vault.fbi.gov/cointel-pro (last visited Mar. 3, 2015).

14. *Id.*

15. Nadia Kayyali, *The History of Surveillance and the Black Community*, ELEC. FRONTIER FOUND. (Feb. 13, 2014), https://www.eff.org/deeplinks/2014/02/history-surveillance-and-black-community (internal quotation marks omitted).

unprecedented glimpse of how the U.S. government watches its citizens—particularly [B]lack citizens."[16] The "Media files" stolen from the FBI office in Pennsylvania in 1971 revealed that African-Americans, FBI Director J. Edgar Hoover's largest targeted group, did not have to be suspected communists, radical, or subversive to become part of the surveillance program, "[n]or was it necessary for them to engage in violent behavior to become a watched person. Being black was enough."[17] The Media files also exposed specific FBI directives to watch Black people wherever they went—in schools, colleges, bars, restaurants, churches, or even outside of their homes.[18]

The brutal mistreatment of Black Americans, as described years ago by Judge Johnson, regrettably continues today. Fifty years after Bloody Sunday, civil rights protests that call attention to the mistreatment of Black citizens in America still occur. On December 16, 2014, thousands took to the streets nationwide, including New York, Washington, Boston, San Francisco, and Oakland to protest the recent killings of Trayvon Martin, Michael Brown, Tamir Rice, Eric Garner, and other unarmed Black men[19] who where choked and shot down by police.[20] These demonstrations are chiefly organized and carried out by the activist movement, Black Lives Matter, which originated following George Zimmerman's acquittal in the murder of Trayvon Martin in July 2013.[21]

So long as members of the Black community continue to act "subversively" to combat this mistreatment, there is no reason to believe that government-initiated, mass-surveillance of the Black community—or of any other ethnic or religious minority group on the FBI's radar—will cease.[22] For instance, as *The Nation* described, since 9/11 the FBI has

16. Betty Medsger, *Just Being Black Was Enough to Get Yourself Spied on by J. Edgar Hoover's FBI*, THE NATION (Jan. 22, 2014), http://www.thenation.com/article/178029/just-being-black-was-enough-get-yourself-spied-j-edgar-hoovers-fbi.

17. *Id.*

18. *Id.*

19. Rich Juzwiak & Aleksander Chan, *Unarmed People of Color Killed by Police 1999-2014*, GAWKER (Dec. 8 2014, 2:15 PM), http://gawker.com/unarmed-people-of-color-killed-by-police-1999-2014-1666672349.

20. Ray Sanchez, *Protesting Police Shootings: Demands for Change Sound Out Nationwide*, CNN (Dec. 16 2014), http://www.cnn.com/2014/12/13/us/nationwide-police-protests/.

21. Michael Segalov, *We Spoke to the Activist Behind #BlackLivesMatter About Racism in Britain and America*, VICE (Feb. 2, 2015), http://www.vice.com/read/patrisse-cullors-interview-michael-segalov-188.

22. Arun Kundnani, Emily Keppler & Muki Najaer, *How One Man Refused to Spy on Fellow Muslims for the FBI—and Then Lost Everything*, THE NATION (Oct. 14, 2014), http://www.thenation.com/article/182096/how-one-man-refused-spy-fellow-muslims-fbi-and-then-lost-everything; *Civil Rights Groups Ask Administration to Explain NSA Surveillance of*

aggressively recruited informants among Muslim communities to gather information regarding community activism efforts, "[b]ut the tactics also fit a familiar pattern—one that harkens back to the FBI's history of targeting the civil rights and Black Power movements of the 1960s."[23]

The Black Lives Matter campaign has the potential to be the next biggest civil rights movement of American history.[24] However, as history has shown, agencies like the NSA and the Department of Homeland Security heighten their surveillance of vaguely defined subversive groups during periods of resistance in the name of protecting national security. If history truly repeats itself, and periods of subversion are followed by mass surveillance, this should be alarming for young activists.

Through the historical framework of the FBI's COINTELPRO activities, this note will argue that civil rights demonstrations today should include direct action against cybersecurity legislation to ensure that the civil liberties of those individuals belonging to marginalized groups are adequately protected in the digital era. This note suggests that civil rights activists should learn from the technology-sector initiated anti-Stop Online Piracy (SOPA) Act and anti-Protect Intellectual Property (PIPA) Act[25] demonstrations of 2012, but should not rely on technology giants to defend their rights within proposed unconstitutional cybersecurity legislation. For reasons explained in more detail below, this note focuses specifically on calling activists' attention to the Cyber Intelligence Protection and Sharing Act ("CISPA").[26]

Part II of this note will provide an overview of CISPA, illustrating the especially damaging effects that this proposed bill may have on our privacy as members of the general public. Part III will discuss the successful activism around the anti-SOPA bills, but will highlight the reality that while technology companies had reason to spearhead that battle, they will

American Muslims, ACLU (July 9, 2014), https://www.aclu.org/national-security/civil-rights-groups-ask-administration-explain-nsa-surveillance-american-muslims.

23. *Id.*

24. Many news sources have argued that the Black Lives Matter Campaign is more sizable than the 1960s and 1970s Civil Rights Movement due to its inclusivity of protestors of all identities, its grassroots, decentralized framework, and its use of modern social media platforms to reach a wide audience. *See generally* Frederick C. Harris, *The Next Civil Rights Movement?*, DISSENT MAGAZINE (2015), https://www.dissentmagazine.org/article/black-lives-matter-new-civil-rights-movement-fredrick-harris; Elizabeth Day, *#BlackLivesMatter: The Birth of a New Civil Rights Movement*, THE GUARDIAN (July 19 2015), http://www.theguardian.com/world /2015/jul/19/blacklivesmatter-birth-civil-rights-movement.

25. This note will use "anti-SOPA campaign," or "stop-SOPA campaign" to refer to the actions taken against both SOPA and PIPA, given that SOPA was the more well-known of the two bills during the online demonstrations of 2012.

26. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (2011–2012) [hereinafter *CISPA*].

have no such motivation to defeat legislation such as CISPA because of the special immunities it provides to these companies. Part IV of this note will strongly suggest that those activists involved in the Black Lives Matter campaign who will likely be under a high level of government scrutiny, take initiative in fighting cybersecurity legislation that has the potential to infringe upon their civil rights. Part IV will propose that civil rights demonstrators should utilize the highly successful strategy crafted and employed by technology companies during the anti-SOPA strikes to effectively stop legislation like CISPA from becoming law.

II. An Overview of CISPA: Surveillance in the Name of Cybersecurity With Technology Company Assistance

In the Internet age, the government employs new methods to watch its citizens. Additionally, governmental surveillance agencies also have an unlikely ally: the technology industry in Silicon Valley. In 2011, Mike Rogers (R-Mich) and Dutch Ruppersberger (D-MD.) introduced CISPA to "[a]mend . . . the National Security Act of 1947 to add provisions concerning cyber threat intelligence and information sharing."[27] CISPA would enable social media platforms and other technology companies to send information related to cybersecurity threats to the Department of Homeland Security ("DHS") and to send information related to "cybercrimes" to the Department of Justice ("DOJ"). CISPA would further allow a company to spy on and share users' sensitive personal information with anyone, including intelligence agencies like the National Security Agency (NSA).[28]

Despite President Obama's veto threat, on April 26, 2012, the House nonetheless passed CISPA by a vote of 248-168,[29] but it later failed in the Senate.[30] In 2013, the House tried again, voting 288-127 in favor of the bill, but the Senate did not even look at it, and the Act died once more.[31] Lawmakers and digital rights groups—including the Electronic Frontier Foundation, the American Civil Liberties Union, the Center for Democracy and Technology, and The Constitution Project—expressed concerns that, as

27. *Id.*

28. Mark Jaycox, *CISPA Passes Out of the House Without Any Fixes to Core Concerns*, ELEC. FRONTIER FOUND. (May 1, 2013), https://www.eff.org/deeplinks/2013/04/cispa-passes-out-house-without-any-fixes-core-concerns.

29. *Comparison of Information Sharing, Monitoring and Countermeasures Provisions in the Cybersecurity Bills*, CTR. FOR DEMOCRACY AND TECH. (July 29, 2012), https://www.cdt.org/files/pdfs/CyberSec_infosharechart_20120730.pdf.

30. Kate Cox, *Third Time's the Charm? House to Take Another Stab at Terrible CISPA Bill*, THE CONSUMERIST (Jan. 8, 2015), http://consumerist.com/2015/01/08/third-times-the-charm-house-to-take-another-stab-at-terrible-internet-bill-cispa/.

31. *Id.*

written, CISPA would allow the government to infringe on citizens' privacy and demand access to personal information such as emails and Internet history without first obtaining search warrants or following other legal procedures.[32]

Representative Dutch Ruppersberger—a staunch advocate for the NSA—is using the recent Sony Hack[33] as an opportunity to reintroduce CISPA to make it easier for the NSA to access data from tech companies.[34] It is also worth noting that Representative Ruppersberger serves as a representative of the Maryland district, home to the NSA's Fort Meade headquarters,[35] which may explain or inform his pro-CISPA opinion.

In the 114th session of Congress, beginning on January 3, 2015, CISPA made another appearance.[36] The list of supporters in 2012 included over 800 companies,[37] including technology companies such as Facebook and Microsoft.[38] These companies supported the measure "because . . . it provides a simple and effective way to share important cyber threat information with the government"[39] and there is no reason to believe that technology companies will withdraw their support anytime soon.

In fact, CISPA 2015[40] "would provide for an even cozier relationship between Silicon Valley and the U.S. government at the detriment of civil liberties and privacy for everyone else."[41] Under the proposed law, Internet companies would "have blanket immunity for feeding the government vaguely-defined 'threat indicators'—anything from users' online habits to the contents of private e-mails—creating a broad loophole in all federal and

32. *Id.*; *see also* Andrew Couts, *CISPA Supporters List: 800+ Companies That Could Help Uncle Sam Snag Your Data*, DIGITAL TRENDS (Apr. 12, 2012), http://www.digitaltrends.com/web/cispa-supporters-list-800-companies-that-could-help-uncle-sam-snag-your-data/.

33. *See* Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Mar. 2015), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

34. Mike Masnick, *Hey Everyone CISPA Is Back. . .Because of the Sony Hack, Which It Wouldn't Have Prevented*, TECHDIRT (Jan. 9, 2015, 9:13 AM), https://www.techdirt.com/articles/20150108/16595129639/hey-everyone-cispa-is-back.shtml.

35. Spencer Ackerman, *Top Democrat on House Intelligence Panel Offers New NSA Reform Plan*, THE GUARDIAN (Mar. 14, 2014), http://www.theguardian.com/world/2014/mar/14/nsa-reform-proposal-house-intelligence-committee-ruppersberger.

36. *Id.*

37. Couts, *supra* note 32.

38. *Id.*

39. Hayley Tsukayama, *CISPA: Who's For It, Who's Against It, and How It Affects You*, WASH. POST (Apr. 27, 2012), http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html.

40. Rachael Tackett, *Exclusive: A Sneak Peak at CISPA 2015*, THE PIRATE TIMES (Jan. 13, 2015), http://piratetimes.net/exclusive-a-sneak-peek-at-cispa-2015/.

41. Kit Daniels, *Lawmaker Reintroduces CISPA Cybersecurity Bill*, INFO WARS (Jan. 15, 2015), http://www.infowars.com/lawmaker-reintroduces-cispa-cybersecurity-bill/.

state privacy laws and even in private contracts and user agreements."[42] The text provides, in relevant part:

> No civil or criminal cause of action shall lie or be maintained in Federal or State court against a protected entity, self-protected entity, cybersecurity provider, or an officer, employee, or agent of a protected entity, self-protected entity, or cybersecurity provider, acting in good faith.[43]

Moreover, although the intent of CISPA is to amend the NSA so that it may collect private information for "cybersecurity purposes" only,[44] once the government has an individual's information, it "can use [that individual's] personal information for cybersecurity . . . *or* [to] protect . . . the national security of the United States."[45]

The FBI has taken extreme measures in the interest of preserving "national security"; COINTELPRO perhaps serves as the most extreme example.[46] However, as one Final Senate Report from 1976 states, the "FBI resorted to counterintelligence tactics in part because its chief officials believed that the existing law could not control the activities of certain dissident groups and that court decisions had tied the hands of the intelligence community.[47] Legislation like CISPA is therefore all the more distressing for members of the American public who desire to engage in politically unpopular behavior because it is distinct in one very important way: COINTELPRO acted alone, deliberately outside the bounds of established law. With the passage of CISPA, however, NSA-led surveillance would be entirely legal: "Unlike Hoover's activities, the NSA's programs come to us with the seal of congressional and judicial approval."[48]

42. Julian Sanchez, *CISPA's Dead. Now Let's Do A Cybersecurity Bill Right*, WIRED (Apr. 26, 2013, 4:55 PM), http://www.wired.com/2013/04/cispas-dead-now-lets-resurrect-it/.

43. H.R. 234, 114th Cong. (2015), https://www.congress.gov/114/bills/hr234/BILLS-114hr234ih.pdf.

44. *Id.*

45. Mark Jaycox & Kurt Opsahl, *CISPA Is Back: FAQ on What It Is and Why It's Still Dangerous*, ELEC. FRONTIER FOUND. (Feb. 25, 2013), https://www.eff.org/cybersecurity-bill-faq.

46. Beverly Gage, *What an Uncensored Letter to M.L.K. Reveals*, N.Y. TIMES MAGAZINE (Nov. 11, 2014), http://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html?_r=1; *see* SENATE SELECT COMM., *supra* note 1, at 10.

47. *See* SENATE SELECT COMM., *supra* note 1, at 10.

48. Beverly Gage, *Somewhere, J. Edgar Hoover is Smiling*, SLATE (June 7, 2013), http://www.slate.com/articles/news_and_politics/history/2013/06/prism_j_edgar_hoover_would_have_loved_the_nsa_s_surveillance_program_topic.html.

CISPA was introduced in the House of Representatives on January 8, 2015, but since then, it has not moved out of the committee stage, and no further action has been taken.[49] However, on March 17, 2015, a similar cybersecurity bill,[50] the Cybersecurity Information Sharing Act ("CISA"), was introduced in the Senate, and on October 27, 2015, the Senate overwhelmingly passed CISA.[51] CISA, like CISPA, creates a program at the DHS that allows private industry to share large quantities of user data with several U.S. government agencies including the NSA,[52] in exchange for complete immunity from Freedom of Information Act ("FOIA") requests and any regulatory action arising from the data companies have shared. Thus, by providing certain immunities, CISA, if passed by the House of Representatives, similarly incentivizes private industry to share the personal data that those companies mine—from email content,[53] to credit card statements, prescription drug records, or target advertising information—with the government, which has previously not had access to such information.[54] And, like CISPA, CISA allows companies to share information with the government for similarly vague and overbroad reasons, that is, if the information contains any "cyber threat indicators."[55]

In contrast to CISPA, security researchers, and even some technology companies, displayed public opposition to CISA, including Apple and Dropbox, proclaiming that CISA invaded their customers' privacy. But Facebook, Microsoft, and Google have been publicly silent about their stance on the bill, as they were during CISPA 2012 debates,[56] even though trade associations representing these companies have publicly objected to CISA.[57] *The Guardian* has reported that such technology industry giants may not be publicly opposed because they already have their own threat-sharing programs, and FOIA immunity, as provided by CISA, could be

49. Actions Overview of H.R. 234, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/234/actions (last visited Oct. 28, 2015).

50. Trevor Timm, *The Senate, Ignorant on Cybersecurity, Just Passed a Bill About It Anyway*, THE GUARDIAN (Oct. 27, 2015), http://www.theguardian.com/commentisfree/2015/oct/27/senate-ignorant-of-cyber-security-just-passed-cisa-bill-anyway ("The bill, which used to be known as Cispa, has been festering in Congress for years, and now it looks like it will finally head to the President's desk.").

51. Sam Thielman, *Senate Passes Controversial Cybersecurity Bill CISA 74 to 21*, THE GUARDIAN (Oct. 27, 2015), http://www.theguardian.com/world/2015/oct/27/cisa-cybersecurity-bill-senate-vote.

52. Timm, *supra* note 50.

53. *Id.*

54. Thielman, *supra* note 51.

55. Timm, *supra* note 50.

56. *See* Couts, *supra* note 32.

57. Thielman, *supra* note 51.

useful to them.[58] The conference committee between the House of Representatives and the Senate will determine CISA's final language.[59]

For outspoken minority groups today, bills like CISPA and CISA should be especially alarming, given the U.S. government's history of surveillance of so-called "subversive" groups during times of turmoil.[60] One might also argue that the lack of minority representation in the cybersecurity industry renders these populations more vulnerable to privacy abuses because there would be even less top-down incentive for checks and balances.[61] A cybersecurity diversity amendment to H.R. 4061, the "Cybersecurity Enhancement Act," proposed by Congressman Alcee L. Hastings (D-Fla.) overwhelming passed through the House in 2010.[62] Nonetheless, minorities remain highly underrepresented, as they are in all science, technology, engineering, and mathematics ("STEM") professions.[63]

Thus, in the wake of recent protests calling attention to the structural racism in American society, this author encourages civil rights activists to incorporate cybersecurity legislative demonstration and reform efforts into the Black Lives Matter movement.

A. Examples of Increased Surveillance During Black Lives Matter Protests

When the grand jury declined to indict Officer Darren Wilson,[64] one of the largest Ferguson-related protests in the country erupted. As the *Boston Herald* reported in November 2014, law enforcement officials at the DHS

58. *Id.*

59. Mark Jaycox, *EFF Disappointed as CISA Passes Senate*, ELEC. FRONTIER FOUND. (Oct. 27, 2015), https://www.eff.org/deeplinks/2015/10/eff-disappointed-cisa-passes-senate.

60. Seth Rosenfeld, *New FBI Files Show Wide Range of Black Panther Informant's Activities*, REVEAL: THE CTR. FOR INVESTIGATIVE REPORTING (June 9, 2015), https://www.revealnews.org/article/new-fbi-files-show-wide-range-of-black-panther-informants-activities/ (indicating that newly released FBI records reveal that the FBI employed informants to spy on Black Panther activities between 1961 and 1971); *Red Scare*, THE HIST. CHANNEL, http://www.history.com/topics/cold-war/red-scare (stating that J. Edgar Hoover's FBI compiled several files on suspected communists through the use of wiretaps and surveillance during the Red Scare).

61. *Cybersecurity Diversity Amendment Overwhelmingly Passes House*, MINORITY NEWS (Mar. 6, 2015), http://www.blackradionetwork.com/cybersecurity_diversity_amendment_overwhelmingly_passes_house.

62. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. (2009–2010), https://www.congress.gov/bill/111th-congress/house-bill/4061/amendments.

63. NAT'L CTR. FOR SYS. SEC. AND INFO. ASSURANCE (CSSIA), http://www.cssia.org/cssia-outreach.cfm (last visited Oct. 24, 2015).

64. *So-called 'Counterterror' Fusion Center in Massachusetts Monitored Black Lives Matter Protesters*, PRIVACY SOS (Nov. 28, 2014, 2:53 PM), https://privacysos.org/node/1603; *see also* Antonio Planas, *As Evans Lauds Boston Cops, Some Protestors Cry Foul*, THE BOSTON HERALD (Nov. 27, 2014), https://www.bostonherald.com/news_opinion/local_coverage/2014/11/as_evans_lauds_boston_cops_some_protesters_cry_foul.

funded "Commonwealth Fusion Center" spied on the Twitter and Facebook accounts of those protestors involved. There are 100 Fusion Centers[65] nationwide, and the two located in Massachusetts relied heavily on "counterterrorism" grants. The ACLU of Massachusetts, and the National Lawyers Guild's Massachusetts Chapter disclosed internal "intelligence files" showing that Boston officials used their federally funded "counterterrorism" infrastructure to monitor nonviolent protestors, labeling them as "domestic extremists" and "homeland security threats."[66]

On December 20, 2014, Black Lives Matter protestors gathered at Mall of America in Minneapolis.[67] On February 2, 2015, attorneys representing Black Lives Matter Minneapolis obtained a copy of a warrant from the Bloomington Police Department granting the police permission to seize private information from Nick Espinosa's Facebook account.[68] Espinosa, a community activist who participated in the Occupy Minnesota movement,[69] was also discussed in a complaint filed by the State of Minnesota charging attorney Nekima Valdez Levy-Pounds with trespass, unlawful assembly, and public nuisance violations among other causes of action.[70] The complaint discusses how Bloomington Police were "alerted to the existence of a Facebook webpage purporting to organize a large scale demonstration being organized by a group identifying itself as 'Black Lives Matter' and used the page, and publicly-available information on Espinosa's Twitter account to infiltrate protests dressed in 'plain clothes.'"[71] Espinosa issued a public statement after learning about the warrant for his Facebook account information stating, "[t]he blatant violation of [his] privacy and civil rights [was] part of an ill-conceived crusade by the City of Bloomington to

65. Kara Dansky, *Senate Homeland Security Committee Misses the Mark with Statement on DHS "Fusion Center" Program*, ACLU (Oct. 10, 2012), https://www.aclu.org/blog/technology-and-liberty-criminal-law-reform-national-security-free-speech/senate-homeland ("Fusion Centers are state-run collaborations of law enforcement and other public agencies that collect information, including about private citizens, which they then share with each other, with the federal government, and often with the private sector. According to DHS's website, fusion centers are owned and operated by state and local entities with support from federal partners in the form of deployed personnel, training, technical assistance, exercise support, security clearances, connectivity to federal systems, technology, and grant funding.").

66. *Policing Dissent Reports: Boston Police Department "Intelligence Reports" on First Amendment Activity*, ACLU, http://www.aclum.org/policing_dissent/reports (last visited Mar. 6, 2015).

67. *Police Seize Private Facebook Account Info in Black Lives Matter Case*, FIGHT BACK! NEWS (Feb. 4, 2015), http://www.fightbacknews.org/2015/2/4/police-seize-private-facebook-account-info-black-lives-matter-case.

68. *Id.*

69. *Nick Espinosa*, THE UPTAKE, http://theuptake.org/tag/nick-espinosa/ (last visited Mar. 2 2015).

70. Minnesota v. Levy-Pounds, 2015 WL 243617 (Minn. Dist. Ct. 2015).

71. *Id.*

intimidate and silence young activists of color at the behest of the largest shopping mall in the U.S., with our own public dollars."[72] He urged the department to "[e]nd [the] political witch hunt [and] [d]rop the charges . . . ."[73]

In addition, protesters in New York responding to the grand jury's decision not to indict the police officer responsible for the choking death of Eric Garner might be particularly vulnerable to Internet surveillance. The New York Police Department ("NYPD") has increased its use of Internet surveillance tools, including social media, to monitor protestors in recent years.[74] In November 2014, the NYPD announced that it planned to ramp up its social media monitoring to find "lone wolf terrorists" as part of its 9/11-era Operation Sentry Program.[75] The NYPD has even added a facial recognition unit dedicated to scouring Twitter, Facebook, and Instagram to identify suspects.[76] For example, in the Occupy Wall Street ("OWS") protests of 2012, the NYPD monitored organizers' social media accounts. Twitter, fearing that District Court Judge Matthew Sciarrino Jr. would place the company in contempt or face hefty fines,[77] was forced to give up the account of an Occupy protester who was charged with disorderly conduct for blocking the Brooklyn Bridge.[78]

In finding that Twitter's motion to quash the subpoena for OWS protestor's account information was "#denied,"[79] Judge Sciarrino noted that, "[t]he widely believed (though mistaken) notion that any disclosure of a user's information would first be requested from the user and require approval by the user is understandable, but wrong."[80] While Judge

72. *See* Fight Back! News, *supra* note 67.

73. *Id.*

74. Lauren C. Williams, *How NYPD Surveillance Could Affect Eric Garner Protests*, THINK PROGRESS (Dec. 6, 2014, 10:21 AM), http://thinkprogress.org/justice/2014/12/06/3600158/nypd-social-media-eric-garner-protests/.

75. Christian Dolmetsch, *NYPD Says Social Media Monitoring to Rise After Attack*, BLOOMBERG BUS. (Nov. 6, 2014, 2:11 PM), http://www.bloomberg.com/news/articles/2014-11-06/nypd-says-social-media-monitoring-to-rise-after-attack?hootPostID=75e1bc9b295975ba12162947bf993626.

76. Murray Weiss, *High-Tech NYPD Unit Tracks Criminals Through Facebook and Instagram Photos*, DNAINFO (Mar. 25, 2013, 7:08 AM), http://www.dnainfo.com/new-york/20130325/new-york-city/high-tech-nypd-unit-tracks-criminals-through-facebook-instragram-photos.

77. Hanni Fakhoury, *UPDATE: NY Judge Tries to Silence Twitter on Its Ongoing Battle to Protect User Privacy*, ELEC. FRONTIER FOUND. (Sept. 14, 2012), https://www.eff.org/deeplinks/2012/09/ny-judge-tries-silence-twitter.

78. Sean Gardiner, *Twitter Turns Over Occupy Wall Street Tweets*, WALL ST. J.: METROPOLIS BLOG (Sept. 14, 2014, 5:02 PM), http://blogs.wsj.com/metropolis/2012/09/14/twitter-turns-over-occupy-wall-street-tweets/.

79. People v. Harris, 36 Misc. 3d 613, 615 (N.Y. Crim. Ct. Apr. 20, 2012).

80. *Id.* at 618.

Sciarrino in the OWS/Twitter case may be correct that users should not equate privacy of social networking sites with the privacy of their personal homes, this does not mean that Internet users are entitled to *no* privacy protection. For example, the Electronic Frontier Foundation ("EFF") argued in its amicus brief supporting Twitter's motion to quash, "[t]he D.A.'s attempt to obtain all of [the protestor's] information through a subpoena, without first obtaining a warrant, violates [his] First and Fourth Amendment rights, as well as his corresponding rights under the New York Constitution."[81]

Cognizant of the fact that a warrant would still be necessary in certain circumstances, Judge Sciarrino ultimately denied Twitter's motion in part and granted the motion in part.[82] Sciarrino found that under the Stored Communications Act ("SCA"),[83] providers of Electronic Communication Service ("ECS")[84] storing temporary "electronic storage" content information[85] less than 180 days old may only disclose requested information pursuant to a search warrant.[86] The Judge additionally found that "the non-content records such as subscriber information, logs maintained by the network server, etc. and the September 15, 2011, to December 30, 2011 tweets [were] covered by the court order. However, the government must obtain a search warrant for the December 31, 2011, tweet."[87]

Arguably, because proposed legislation like CISPA is designed to make sharing between social media platforms and the government much easier, there would never be need for a judge to issue a warrant. Using the judiciary process to determine whether or not a search was constitutional not only assures Americans that their rights are not being violated, but it also makes visible the fact that an issue of law exists in the first place. By ensuring that the transfer of personal data happens in a very non-

81. Brief for ACLU et al., as Amici Curiae Supporting Respondent at 1, *Harris*, 36 Misc. 3d 613 (N.Y. Crim. Ct. Apr. 20, 2012) (No. 2011NY080152), 2012 WL 2885909.

82. People v. Harris, 36 Misc. 3d 868, 878 (N.Y. Crim. Ct. June 30, 2012).

83. *Id.* at 868.

84. Electronic communications service (ECS) is broadly defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). It is well-settled that Internet Service Providers (ISPs) qualify as ECS Providers, or ECSPs. *See In re* Doubleclick Inc., 154 F. Supp. 2d 497, 511 n.20 (S.D.N.Y. 2001) (suggesting that "ISPs such as America Online, Juno and UUNet, as well as, perhaps, the telecommunications companies whose cables and phone lines carry the traffic" are ECSPs); Freedman v. America Online, Inc., 303 F. Supp. 2d 121, 124 (D. Conn. 2004).

85. "Content information" in this case refers to actual tweets. *See Harris*, 36 Misc. 3d at 876.

86. Stored Communications Act, 18 USC § 2703(a); *Harris*, 36 Misc. 3d at 876.

87. *Harris*, 36 Misc. 3d at 876–77.

transparent way, CISPA also removes and renders moot this legal mechanism for keeping government agencies accountable.

Privacy rights groups such as the EFF[88] have made aggressive calls to Congress, and to the public at large, to encourage Congress to incorporate crucial provisions into CISPA that would safeguard citizens' civil liberties.[89] Despite these calls to action, Congress has not made the necessary, privacy-protecting amendments to CISPA. Additionally, the public's response to such calls was relatively benign when compared with other Internet actions such as the Stop SOPA campaign, as described below.

This note will now address the Internet activism which took place during the legislature's effort to pass the SOPA and PIPA bills to illustrate two main points. First, activists interested in preserving privacy rights should not rely on technology companies to protect our Constitutional rights. Secondly, there are important lessons regarding the orchestration of an effective Internet demonstration campaign to be learned from the Stop SOPA campaign, which can aid anti-CISPA activists looking to defeat the bill for good.

III. We Should Not Rely on Technology Companies to Defend Our Civil Liberties

A. The Stop SOPA Campaign Revealed: Silicon Valley Uses Unsuspecting Internet Users to Reduce Their Own Liability and Regulatory Compliance Costs

In the Intellectual Property ("IP") world, it is common knowledge that the traditional "writers of copyright's history"[90] are powerful interest

88. *CISPA Is Back*, ELEC. FRONTIER FOUND. https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=9137 (last visited Mar. 2, 2015); *see also* Daniel Jabbour, *Protect Internet Privacy, Stop CISPA!*, CHANGE.ORG, https://www.change.org/p/protect-internet-privacy-stop-cispa (last visited Mar. 6, 2015).

89. *See CISPA Is Back*, ELEC. FRONTIER FOUND., *supra* note 88.

90. It has long been determined by countless academics that the IP system—specifically the copyright regime—represents a legal sphere wherein policies have traditionally been shaped by the political interests of the few. *See generally* Lyman Ray Patterson, *Copyright and "The Exclusive Right" of Authors*, 1 J. OF INTELL. PROP. 1, 13 (1993), http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1342&context=fac_artchop (regarding the passage of the Statute of Anne in England, Copyright Act of 1709: "Booksellers concentrated on the source of copyright in order to turn a legal question into a political question. They did so by arguments intended to elicit sympathy for the author . . . . The right of assignment was the political ploy, for it meant that both the authors could be deprived of their 'natural law' rights by contract, and that the booksellers' monopoly would be enhanced by that same contract."). Such US-based interest groups include the Motion Picture Association of America ("MPAA") (comprised of 6 big media companies: GE, Disney, Newscorp, TimeWarner, Viacom and CBS), the Recording Industry Association of America ("RIAA"), and large software firms who actively lobby on their behalf.

groups in the entertainment industry, and, as a result, ordinary citizens lack the political firepower to influence copyright debates. Thus, just as political scientists and analysts were enthused by the citizen-led "Arab Spring" and its unprecedented transformation of the Middle East and North Africa region,[91] IP scholars were similarly shocked when the copyright regime supposedly experienced *its* first phenomenon in collective action.

In early 2012, digital activism supposedly halted the passage of the Stop Online Piracy Act ("SOPA")[92] and the Protect Intellectual Property Act ("PIPA")[93] in the United States.[94] SOPA was introduced by House Representative Lamar Smith (R-TX) in October of 2011. The bill was the House's version of the Senate's PIPA, or S.968, introduced and authored by Senator Patrick Leahy (D-VT) earlier that May. Both bills responded to U.S. copyright owners' requests for increased protection against infringement committed by foreign websites, which profited from broadcasting American copyrighted content. As expected, SOPA and PIPA received an overwhelming amount of support from "content industry" associations that represent large media conglomerates such as the Motion Picture Association of America ("MPAA"), the Recording Industry Association of America ("RIAA"), American Society of Composers, Authors and Publishers ("ASCAP"). Additionally, both bills were supported by a wide array of business and labor organizations[95] including,

See generally MONICA HORTEN, A COPYRIGHT MASQUERADE: HOW CORPORATE LOBBYING THREATENS ONLINE FREEDOMS (2013).

91. One Harvard academic has written that ICTs generally, and that "Twitter, in particular," had "proven particularly adept at organizing people and information." Jonathan Zittrain, *The Future of the Internet and How to Stop It* (2008). The *Wall Street Journal* went so far as to say that the Twitter-powered "Green Revolution" had, in Iran at least, transformed the Islamic Republic more effectively than "years of sanctions, threats and Geneva-based haggling put together." *The Clinton Internet Doctrine*, WALL ST. J. (Jan. 23, 2010), http://www.wsj.com /articles/SB10001424052748704320104575014560882205670. Other journalists likewise credited social media platforms for doing more for progressive Arab politics than either the U.N. or the European Union. *See generally* S. Spier, *Collective Action 2.0: The Impact of ICT-based Social Media on Collective Action—Difference in Degree or Difference in Kind?*, SOC. SCI. RESEARCH NETWORK (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1979312.

92. Cybersecurity Enhancement Act of 2010, H.R. 4061, 111th Cong. (2009–2010), https://www.congress.gov/bill/111th-congress/house-bill/4061/amendments; Stop Online Privacy Act, H.R. 3261, 112th Cong. (2011) [hereinafter *SOPA*], https://www.congress.gov/112 /bills/hr3261/BILLS-112hr3261ih.pdf.

93. Protect IP Act of 2011, S. 968, 112th Cong. (2011), https://www.congress.gov/ 112/bills/s968/BILLS-112s968rs.pdf

94. Lawrence Lessig, *After the Battle Against SOPA—What's Next?*, THE NATION (Jan. 26, 2012), http://www.thenation.com/article/165901/after-battle-against-sopa-whats-next#; Chris Civil, *When the Net Went Dark: SOPA, PROTECT IP and the Birth of an Internet Movement*, BERKELEY TECH. L.J. (Feb. 2012),http://btlj.org/2012/02/14/when-the-net-went-dark-sopa-protect-ip-and-the-birth-of-an-interent-movement/.

95. The list of SOPA supporters includes American Federation of Labour and Congress of Industrial Organizations ("AFL-CIO"). *See* Connor Adams Sheets, *SOPA Supporters:*

but not limited to, pharmaceutical and cosmetic companies,[96] which were similarly motivated by the economic importance of U.S.-created IP.

The bills did, however, receive harsh criticism from many digital rights advocacy groups, major technology companies such as Google, Facebook, and Twitter, online payment providers, and IP scholars. SOPA and PIPA had the potential to affect a multitude of tech companies in Silicon Valley in disastrous ways.[97] Web 2.0 platforms, by design, are especially reliant upon user-generated content ("UGC") to function; the text of SOPA could have forced the wholesale shutdown of sites even if just one user were to post content protected under U.S. copyright law.[98] PIPA limited its private IP-owner right of action by requiring him or her to refer to the federal court system to bring a suit against any domestically or internationally-registered domain name server ("DNS").[99] In contrast, under SOPA, IP rights holders could initiate proceedings against both US and foreign-based websites as outlined in Section 103.[100] Since ISPs would be liable for infringing content in the event the site is found guilty, there would be no incentive for them to keep material available. Fred Wilson, Principal of Union Square Ventures, expressed concern that SOPA in particular would alter the Digital Millennium Copyright Act ("DMCA") safe-harbor landscape which undoubtedly encouraged start-up companies like Facebook, Twitter, Dropbox, Netflix and Spotify to take initial investment risks.[101] With legislation like SOPA, Wilson contends that creative entrepreneurs in the lucrative technology sector would instead think twice about creating their businesses because more capital would go to defense attorneys than innovative software engineers,[102] a concern also shared by the EFF.[103]

Companies and Groups that Support the Controversial Bill, INT'L BUS. TIMES (Jan. 5, 2012), http://www.ibtimes.com/sopa-supporters-companies-groups-support-controversial-bill-391250.

96. Supporters also include Pharmaceutical Research and Manufacturers of America, Pfizer, Inc., Revlon, and Loreal Inc. *See id.*

97. Corynne McSherry, *SOPA: Hollywood Finally Gets a Chance to Break the Internet*, ELEC. FRONTIER FOUND. (Oct. 28, 2011), https://www.eff.org/deeplinks/2011/10/sopa-hollywood-finally-gets-chance-break-internet.

98. *See id.*; *see also* Civil, *supra* note 94.

99. *See* Civil, *supra* note 94.

100. *Id.*

101. *SOPA*, *supra* note 92. Title II of SOPA, or "Additional Enhancements to Combat Intellectual Property Theft," went further by strengthening legislation such as the Commercial Felony Streaming Act (CFSA) which focuses on streaming content in particular. *Id.*

102. Fred Wilson, *Protecting the Safe Harbors of the DMCA and Protecting Jobs*, AVC (Oct. 29, 2011), http://www.avc.com/a_vc/2011/10/protecting-the-safe-harbors-of-the-dmca-and-protecting-jobs.html.

103. Peter Eckersley & Corynne McSherry, *Hollywood's New War on Software Freedom and Internet Innovation*, ELEC. FRONTIER FOUND. (Nov. 11, 2011), https://www.eff.org/deeplinks/2011/11/hollywood-new-war-on-software-freedom-and-internet-innovation.

Kent Walker, the Senior Vice President of Google, provided Congressional testimony that "DNS blocking itself could affect the Internet's reliability, security, and performance."[104] This apprehension was reiterated in a letter opposing PIPA addressed to the members of Congress sent in July 2011. In the letter, 108 professors in the U.S. legal community, including notable professors Mark Lemley and Lawrence Lessig, criticized the bill for presenting "[d]ifficult enforcement challenges . . . grave constitutional infirmities, potentially dangerous consequences for the stability and security of the Internet's addressing system" and concluded that it would ultimately "undermine [U.S.] foreign policy and strong support of free expression on the Internet around the world" if the bill were passed.[105] SOPA and PIPA were essentially characterized in the same vein as the French HADOPI law,[106] which was described by opponents as disproportionate, out of touch and detrimental to the progression of the digital world.[107] SOPA, especially, required a lot of tech companies' support, financiallyspeaking. The draconian obligations foisted upon ISPs, financial services firms, advertisers, and search engines meant that these companies would have to consult an ever-growing list of prohibited sites

104. *Google Testimony on Online "Promoting Investment and Protecting Commerce Online,"* INFOJUSTICE.ORG (Apr. 6, 2011), http://infojustice.org/archives/2965.

105. *Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (PROTECT IP Act of 2011, S. 968)*, https://www.wyden.senate.gov/download/?id=82557539-159c-4237-b6a0-27d0d43b7797&download=1 (last visited Oct. 29, 2015).

106. The media content industry's failure to fully embrace and adapt to new technologies has culminated into increasingly hostile and excessive retaliatory responses; extensive lobbying on their part has produced "graduated response" or "three-strikes" laws around the world where ISPs are compelled to disconnect users after receiving a few written warnings from copyright holders. *See* Brett Danaher, Michael D. Smith, Rahul Telang, & Siwen Chen, *The Effect of Graduated Response Anti-piracy Laws on Music Sales: Evidence from an Event Study in France*, SOC. SCI. RESEARCH NETWORK (Jan. 2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240; Eric Pfanner, *France Approves Wide Crackdown on Net Piracy*, N.Y. TIMES (Oct. 22, 2009), http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1. France became the first country to implement legislation of this sort when in May of 2009 the French Parliament passed HADOPI, or the Creation and Internet Law. Eric Pfanner, *supra*. Despite the criticism HADOPI received from certain members of the European Parliament, the Constitutional Council of France, politicians in the French Socialist and Green parties, activism groups such as La Quadrature du Net, journalists worldwide, and bloggers in the cyber community, HADOPI was nonetheless approved save one key revision: the approved version states that a judge, as opposed to the HADOPI authorizing agency, will be required to sign off on an Internet account suspension. *Id.* This provision does not however, address the aforementioned violations of privacy, human rights, and proportionality affected by the three strikes' law. Danaher et al., *supra*.

107. Rainey Reitman, *Repealing French Three Strikes Law Is the Next Step to Safeguarding Free Expression*, ELEC. FRONTIER FOUND. (Aug. 8, 2012), https://www.eff.org/deeplinks/2012/08/repeal-french-three-strikes-law (citing Boris Manenti, *Aurélie Filippetti: Je vais réduire les crédits de l'Hadopi*, (Aug. 1, 2012), http://o.nouvelobs.com/high-tech/20120801.OBS8587/aurelie-filippetti-je-vais-reduire-les-credits-de-l-hadopi.html).

that they are not allowed to connect to or do business with. This point is critical in understanding *why* Silicon Valley firms strongly opposed SOPA.

The tech companies, in an unprecedented move, encouraged Internet users to lend their support.[108] Rather than engaging in costly lobbying campaigns, Silicon Valley worked diligently to engage the public by appealing to their fears of Internet censorship, thus recruiting unassuming, ordinary Internet users to join their side of the debate.

Their strategically crafted rhetoric was arguably a large part of the U.S. protest's success, given that it shifted the focus away from a company's duty to assume liability for copyright infringement as "gatekeepers" of the Internet and instead made the protest a civil rights issue.[109]

Silicon Valley's opposition became known to the entire online community when, on January 18, 2012, their campaign immediately gained momentum after a well-executed 24-hour "blackout" protest.[110] Popular sites and nonprofit organizations including the Wikimedia Foundation (operator of Wikipedia), Mozilla, and Reddit suspended their operations and instead provided links to inform site users of the reasoning behind their protest. They also encouraged all those opposed to contact their local representatives to speak out against the bills. An estimated 75,000 other websites from around the world also participated in the blackout day.[111] Google restricted its participation in the 'Internet strike' to just blocking out its logo, but it also used the blackout to promote an anti-SOPA petition which collected over 4.5 million signatures. Protestors eventually delivered a petition to lawmakers in Capitol Hill with over 14 million names; more than 10 million of those signatories were ordinary voters.[112] January 18, 2012, marked the largest online protest in history.[113]

The voices of the opposition movement were heard. On January 20, just two days after the blackout, a majority of Congressional leaders in both political parties withdrew their support and indefinitely shelved both anti-

108. SOPA STRIKE, http://www.sopastrike.com/ (last visited Oct. 24, 2015).

109. *See id.* ("January 18th was unreal. Tech companies and users teamed up. Geeks took to the streets. Tens of millions of people who make the internet what it is joined together to defend their freedoms. The network defended itself. Whatever you call it, we changed the politics of interfering with the internet forever—there's no going back.").

110. *Wikipedia Blackout: 11 Huge Sites Protest SOPA, PIPA on January 18*, HUFFINGTON POST (Jan. 18, 2012), http://www.huffingtonpost.com/2012/01/17/wikipedia-blackout_n_1212096.html.

111. *See* Lessig, *supra* note 94.

112. Jonathon Weisman, *After an Online Firestorm, Congress Shelves Antipiracy Bills*, N.Y. TIMES (Jan. 20, 2012), http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html.

113. *See* SOPA STRIKE, *supra* note 108.

piracy bills.[114] In the aftermath of the action, there was much self-congratulating from the Internet participants. *TechCrunch* provides an explanation of the shared sentiment underlying the euphoria as such: "Not a single anti-SOPA lobbyist was hired for yesterday's protest . . . [a] well-organized, well-funded, well-connected, well-experienced lobbying effort on Capitol Hill was outflanked by an ad-hoc group of rank amateurs."[115] The *New York Times* described what happened as an "Online Firestorm" in which "Internet giants rallied their troops to rise up against such Washington stalwarts as the [MPAA] and the [RIAA]."[116] Democratic Senator Ron Wyden stated that the event marked a "new day in the Senate," forever changing the way "citizens communicate with their government."[117] Forbes proclaimed: "One thing is now entirely clear. The Internet won."[118] Popular blog *Techdirt* asserted that "[i]t wasn't Silicon Valley or Google that Stopped SOPA/PIPA, it was the Internet."[119] Annemarie Bridy, Visiting Scholar at Princeton University's Center for Information Technology Policy, also insisted, "[c]ongressional support for SOPA/PIPA quickly evaporated in the face of mass networked resistance."[120] Members of the *Berkeley Technology Law Journal* further added that the activist effort "may represent a key turning point in debates of future copyright legislation and reform."[121] Harvard Law professor and prominent IP scholar Lawrence Lessig commented that this marked the first time in copyright's long history that "the Internet ha[s] taken on Hollywood extremists and won."[122] In short, the Internet was widely held to be *mostly* responsible for changing the course of IP policy-making in this particular instance. The protest of SOPA/PIPA became known to the IP system as what the Arab Spring was to democratic reform in the Middle

114. Julianne Pepitone, *SOPA and PIPA Postponed Indefinitely After Protests*, CNN MONEY (Jan. 20, 2012), http://money.cnn.com/2012/01/20/technology/SOPA_PIPA_postponed/.

115. David Rodnitzky, *Lobbyists 1, Internet 0: An Alternative Take on SOPA*, 3 DIGITAL (Jan. 26, 2012), http://www.ppcassociates.com/blog/experience/lobbyists-1-internet-0-an-alternative-take-on-sopa/.

116. See Weisman, *supra* note 112.

117. *Id.*

118. Larry Downes, *Who Really Stopped SOPA, and Why?*, FORBES (Jan. 25, 2012, 1:15 AM), http://www.forbes.com/sites/larrydownes/2012/01/25/who-really-stopped-sopa-and-why/.

119. Mike Masnick, *Once More, with Feeling: It Wasn't Silicon Valley or Google That Stopped SOPA/PIPA, It Was the Internet*, TECHDIRT (Jan. 26, 2012), http://www.techdirt.com/articles/20120125/10521617539/once-more-with-feeling-it-wasnt-silicon-valley-google-that-stopped-sopapipa-it-was-internet.shtml.

120. Annemarie Bridy, *Copyright Policymaking As Procedural Democratic Process: A Discourse-theoretic Perspective on ACTA, SOPA, and PIPA*, 30 CARDOZO ARTS & ENTM'T L. J. 153, 159–60 (2012).

121. *See* Lessig, *supra* note 94; *See* Civil, *supra* note 94.

122. *See* Lessig, *supra* note 94.

East and North Africa ("MENA") region: utterly unexpected and, given the historical context framing both events, truly revolutionary indeed.

However, it was Silicon Valley's strategic incorporation of skillfully designed discourse that recruited the impressive numbers of cyber-activists to join the campaign and falsely led Internet users to believe [they] alone "[took] on Hollywood extremists and won."[123] During the SOPA and PIPA debates, these tech firms claimed that enacting the bills would censor the Internet and trample on users' freedoms, creating an online environment comparable to China's "Great Firewall."[124]

Google, for instance "watered down the anti-corporate aspects of the campaign"[125] and, "[i]nstead of attacking IP laws and corporate profits, Google stressed the need to preserve innovation, economic growth, and job creation."[126] Google refrained from mentioning its own corporate interest in defeating SOPA and PIPA. The multibillion-dollar company did not mention that the bills would reduce their overall profit and increase their liability as the most popular search engine by asking it to act as a regulator of piracy on the web. Instead, Google promoted the tame, business-friendly, and highly appealing slogan of "End Piracy, Not Liberty."[127]

This discourse not only won the support of Internet users worldwide, but it also provided ordinary citizens with a false sense of empowerment, at least with regard to their capacity to affect copyright policy. This note contends that without the support of technology companies, their enormous lobbying influence in Washington,[128] and their artfully designed rhetoric, it

123. *Id.*

124. Josh Rudolph, *SOPA/PIPA: The Great Firewall of the West? (Updated)*, CHINA DIGITAL TIMES (Jan. 18, 2012), http://chinadigitaltims.net/2012/01/sopapipa-the-great-firewall-of-the-west/.

125. George Martin Fell Brown, *SOPA and PIPA Defeated*, SOCIALIST WORLD (Mar. 4, 2012), http://www.socialistworld.net/print/5645.

126. *Id.*

127. *End Piracy, Not Liberty—Google Millions of Americans Oppose SOPA and PIPA*, YOUTUBE, https://www.youtube.com/watch?v=tXad_E2DcYE (last visited Oct. 28, 2015).

128. David Rodnitzky highlights the fact that when Google, Facebook, and other Internet giants bought full page ads in major newspapers delineating the reasons for their opposition to the bills, Nancy Pelosi (D-Calif.) and Darrell Issa (R-Calif.) came out against the bills almost immediately afterwards. *See* Rodnitzky, *supra* note 115. According to *Open Secrets*, a nonpartisan, independent, and non profit organization whose self-stated mission is to make government more responsive and transparent, Google is the eighth largest contributor to Representative Nancy Pelosi, and Facebook is listed as her fifth largest contributor. *Nancy Pelosi: Top 20 Contributors: 2009–2010*,' OPEN SECRETS (last visited Apr. 25, 2011), http://www.opensecrets.org/politicians/contrib.php?cycle=2010&type=I&cid=N00007360&newmem=N&recs=20; *see also* Nelson Wang, *Google Political Donations: Where Company Execs Put Their Cash*, CBS (updated Sept. 21, 2011), http://www.cbsnews.com/8301-505123_162-46840313/google-political-donations-where-company-execs-put-their-cash/. Darrell Issa is listed as one of Google's top contribution receivers of 2012, perhaps assisting in our understanding of why Issa fervently asserted that lawmakers cannot simply "use Google as a piñata and bash on it"

is not clear that Internet users would have "shelved the bills indefinitely."[129]

B. Self-Interested Technology Companies Supported Anti-Civil Liberties Legislation Behind the Scenes of the Stop SOPA /PIPA Strikes

During the SOPA and PIPA strikes, big tech firms made their support of the web community-friendly OPEN Act[130] well-known, however, they were not as quick to publicize their support of CISPA. Google declined to publicly comment on its position towards the bill, as its support of CISPA would have angered the Internet activists who joined with the company to oppose SOPA. However, just weeks before CISPA passed in the House, Google acknowledged in its latest lobbying disclosure form that it is working behind the scenes on CISPA and supporting the legislation with political donations.[131]

Paralegal.net created an infographic titled "WTF is CISPA" in which it announced that "while protesters were occupied with SOPA, a new cyber-security bill snuck its way into congressional consideration . . . [that] makes SOPA look like amateur hour."[132]

until the piracy problem is eliminated. Peter Voskamp, *Online Piracy Act Dead? Nancy Pelosi, Darrell Issa Both Come Out Against (Updated)*, REUTERS (Nov. 17, 2011), http://www.reuters.com/article/2011/11/17/idUS402801936220111117.

129. *See* SOPA STRIKE, *supra* note 108.

130. In the midst of the SOPA/PIPA debates in January of 2012, Facebook joined AOL, eBay, Google, LinkedIn, Mozilla, Twitter, Yahoo, and other Silicon Valley giants to publicize their support for an alternative bill, The Online Protection and Enforcement of Digital Trade, or the OPEN Act. Wendy Davis, *Silicon Valley Backs Wyden-Issa Approach to 'Rogue' Sites*, THE DAILY ONLINE EXAMINER: POL'Y BLOG (Dec. 14, 2011, 5:41 PM), http://www.mediapost.com/publications/article/164254/silicon-valley-backs-wyden-issa-approach-to-rogue.html. In a letter to congress, these companies claimed that OPEN "[t]argets foreign rogue sites without inflicting collateral damage on legitimate, law-abiding U.S. Internet companies." *Id.* After examining OPEN, the EFF stated that the draft legislation addressed many of the glaring problems associated with SOPA/PIPA. Julie Samuels, *An Alternative to SOPA: An Open Process Befitting an Open Internet*, ELEC. FRONTIER FOUND. (Dec. 8, 2011), https://www.eff.org/deeplinks/2011/12/alternative-sopa-open-process-befitting-open-internet. Interestingly, however, the bill does not require ISPs or search engines to take any action. *Id.* The elimination of liability for these companies perhaps explains tech companies' endorsement of OPEN over SOPA/PIPA. This is not the first time that ISPs have jumped to support an otherwise controversial bill simply because the ISP immunity clause was dropped, and the public should be mindful of this before trusting in corporations to look out for their interests as ordinary citizens. OPEN, for example, lacks what EFF calls a "public interest provision," which would mandate that the ITC take into account the public interest. *Id.* If the balance of power between IP-rights holders and the public's is skewed in favour of the former, any cease and desist order has the potential to benefit an IP holder, or distributer of IP rights, to the detriment of the public's needs.

131. Brenden Sasso, *Google Acknowledges Lobbying on Cybersecurity Bill CISPA*, THE HILL (Apr. 23, 2012), http://thehill.com/blogs/hillicon-valley/technology/223069-google-acknowledges-lobbying-on-cybersecurity-bill-cispa.

132. Ron Miller, *WTF Is CISPA? (Infographic)*, SOC. MEDIA NEWS (May 1, 2012), http://socmedianews.com/2012/05/wtf-is-cispa-infographic/.

Much like SOPA and PIPA, Rogers and Ruppersberger framed CISPA as a bill to protect U.S. intellectual property from digital theft committed by foreign states.[133] However, as explained in the previous section on this paper, CISPA has the potential to have a far more deleterious impact on Internet users' rights than SOPA/PIPA ever could have had. But, because under SOPA/PIPA, tech companies would be held responsible for any IP infringing content, it was in their interest to oppose those bills. On the other hand, CISPA actually *incentivizes* personal data collection and intercepting or modifying user communications by setting up a business-government information sharing system. Firms are encouraged to "share" cyber-intelligence with the U.S. government,[134] and CISPA's Director of National Intelligence passes along threatening information to private companies, which can "protect the rights and property [of protected[135] and self-protected entities]"[136] more effectively.

Put differently, CISPA, unlike SOPA and PIPA, does not threaten Silicon Valley's business interests, and thus tech giants are not motivated to orchestrate a blackout in this case.[137] If tech giants' interests truly aligned with the public interest, then disproportionate legislation like CISPA would be dismissed immediately, given the inclusion of its flagrant privacy-invasive clauses. The same nonprofit digital rights groups and IP scholars who opposed SOPA and PIPA spoke out against CISPA,[138] but could not kill the bill without the financial support of tech companies, and with letter writing campaigns to Congress from grassroots organizations alone.[139] Now, CISPA is back before Congress again for the third time.[140] In a recent speech to Stanford University, President Obama stated that "[t]here's only one way to defend America from cyber threats [such as the Sony Hack] . . . and that is government and industry working together—sharing information—as true partners."[141] While the President was not

133. *See CISPA*, *supra* note 26.

134. *See id.* § 2(b)(1)(B)(ii).

135. A "protected entity" under CISPA may include the federal government. *Id.* § 2 (b)(1)(A)(ii).

136. *See id.* § 2(b)(1)(A), (B).

137. Robert Levine, *Why No Web Blackout for CISPA? Google It*, FAST CO. (May 9, 2012), http://www.fastcompany.com/1836709/why-no-web-blackout-cispa-google-it.

138. Organizations Opposing H.R. 3523, OPEN CONGRESS, https://www.opencongress.org/bill/hr3523-112/bill_positions (last visited Oct. 28, 2015).

139. *Coalition Letter on CISPA*, ACLU, https://www.aclu.org/files/assets/coalition_letter_re_deep_concerns_about_s__2105_-_5_10_12.pdf (last visited Oct. 24, 2015).

140. Shane Blume, *CISPA Back for Third Time*, ETEKNIX, http://www.eteknix.com/cispa-back-third-time/ (last visited Oct. 28, 2015).

141. Dominic Rushe, *White House Warns Tech World That Sony-style Hacks "Could Become the Norm,"* THE GUARDIAN (Feb. 13, 2015), http://www.theguardian.com/us-news/2015/feb/13/white-house-sony-hacking-the-interview.

speaking directly about CISPA, his statement encompassed the essential function of CISPA—to provide greater information sharing between the public and private sectors.

The combination of President Obama's fervent belief that bills like CISPA would enhance national security, and the built-in incentives for tech companies to support such legislation, does not bode well for civil rights activists seeking to stop other deleterious surveillance legislation in its tracks.

As a result, this note recommends that activists launch an aggressive campaign to prevent privacy-eroding anti-surveillance bills from becoming law as an additional, but crucial, effort in the fight to attain civil rights protections for minority communities.

IV. Recommendation That Civil Rights Activists Fight Anti-Surveillance Legislation

Given that CISPA is back again in 2015, civil rights activists—particularly those belonging to communities of color—should certainly begin to think about how to incorporate a true grassroots-initiated Internet campaign to prevent surveillance laws from passing as part of the broader civil rights movement in the wake of Fergusson.

As mentioned in Part II, given the history of the FBI's surveillance of alleged subversive minority groups beginning in the 1950s, minority groups should be especially alert to legislation that seeks to collect mass amounts of information from citizens.

Although, as Part III illustrates, it is unlikely that large technology companies will join activists in the struggle to ensure adequate privacy protections are contained within potential surveillance laws, activists can nonetheless take from the anti-SOPA campaign a successful blueprint for combating such legislation.

A. Using the "SOPA strike" as a guide for anti-CISPA efforts.

Although it is doubtful that Internet activism ultimately defeated SOPA and PIPA, there are still lessons to be learned from the hugely successful rhetorical campaign orchestrated by technology companies.

Alison Powell, an academic at the University of Oxford Internet Institute determined in a recent article that the Jan 18 action was significant in connecting the proposed laws with a discourse of Internet censorship; and amplifying that discourse through online and mass media to provoke a policy response.[142] Powell suggests that the Blackout Day in January, also

142. Alison Powell, *Assessing the Influence of Online Activism on Internet Policy-making: The Case of SOPA/PIPA*, OXFORD INTERNET INST. (2012).

known as the "SOPA strike" or the "Stop SOPA" campaign was not significant solely because it generated people power. Powell asserts that the process of connecting both bills with a no-fail discourse, and then amplifying that discourse on the web to reach thousands of people ultimately made the action particularly significant. This note avers that the approach used by technology companies to garner support for the stop SOPA campaign can be emulated in the Black Lives Matter campaign to indefinitely halt privacy-eroding surveillance legislation like CISPA.

B. A Suggested Online Campaign Strategy

Following the Stop-SOPA campaign strategy, articulated by Alison Powell, Step One would be to connect CISPA with a powerful "no-fail" discourse. Step Two would be to then amplify that discourse on the Internet to reach thousands of people.

The Stop SOPA campaign included such slogans and phrases as "End Piracy, Not Liberty,"[143] these bills could "censor the web,"[144] "We can't endanger an open internet,"[145] and "The American government tries to regulate the Internet like Communist China."[146] Buzzwords like liberty, freedom, openness, censorship, and analogizing U.S. action to extreme communist governments is an effective way to catch people's attention and rouse support.

Likewise, slogans as simple as "Protect Civil Liberties. End CISPA," "Surveillance Compromises Our Freedom," "Preserve the Right to Protest," "#BlackLivesMatter. Stop Surveillance Now," "Our Right to Privacy is Under Threat. Stop CISPA Now," and "Protect the Integrity of the First and Fourth Amendments, Stop CISPA Now," are examples of phrases that might capture an Internet audience's attention. The EFF, ACLU, and other civil rights organizations do a tremendous job of boiling down and explaining complex legislation to the general public; however, the same slogans that immediately drew the attention of the web in 2012 are missing from efforts to stop CISPA. This note contends, as Bridy argues, that this persuasive rhetoric, absent currently, could make a difference when strategizing for the next Internet-led campaign. One Facebook page highlighting awareness of CISPA seems to have the right

143. *What We've Done*, GOOGLE: TAKE ACTION, https://www.google.com/takeaction/past-actions/end-piracy-not-liberty/ (last visited Oct. 24, 2015).

144. *Id.*

145. Senator Jeff Merkley (@SenJeffMerkley), TWITTER (Jan. 18, 2012, 8:47 AM), https://twitter.com/SenJeffMerkley/status/159678431406202881.

146. *The American Government Tries to Regulate the Internet Like Communist China*, NICKSANDLIN.COM: NEWS FOR ENTM'T & TECH. (Apr. 6, 2014), http://nicksandlin.com/2014/04/06/the-american-government-tries-to-regulate-the-internet-like-communist-china/.

idea: its "cover photo" urges the public to "Stand up for Internet freedom. Say no to CISPA."[147] Unfortunately, as of March 6, 2015, the page has only 8,821 "likes," in contrast to the Stop SOPA page, which had at least 53,000 "likes."[148]

Of course, step two would be to amplify the anti-CISPA discourse to evoke a response on the web. Here, critics might argue that the involvement of influential technology companies who were able to "blackout" their pages called most of attention to the issue. This note concedes that this was a huge part of the success of the Stop SOPA campaign. But, as Annemarie Bridy, contends, the rhetorical weaponry created by those companies also provided a crucial ingredient for success. Therefore, this pitfall may be overcome by a rights discourse that effectively motivates the Internet community to take action. Furthermore, as demonstrated by the mass support generated by the Black Lives Matter movement, young people right now are especially interested in civil rights actions. The combined "Justice For All" and "Millions March" protests against police brutality that took place in Washington D.C. and New York on December 13, 2004, were estimated to have included roughly 75,000 people.[149] Thus, there is strong reason to believe that people will support a campaign that aims to protect the civil liberties of those involved in these demonstrations.

Amplifying this discourse on the web, as the world has seen from the Black Lives Matter campaign or even the "Arab Spring" uprising, can be achieved without shutdowns of entire web pages—Twitter has the ability to serve as a very powerful platform for change. For example, Harvard academic Jonathan Zittrain, wrote that information communication technologies generally, and "Twitter, in particular," have "proven particularly adept [during the Arab Spring] at organizing people and information."[150] The *Wall Street Journal* went so far as to say that "the Twitter-powered 'Green Revolution' had, in Iran at least, transformed the Islamic Republic more effectively than 'years of sanctions, threats and

147. *Stop CISPA, the New U.S. Anti-Privacy Bill*, FACEBOOK, https://www.facebook.com/StopTheCISPA (last visited Oct. 24, 2015).

148. *Stop SOPA*, FACEBOOK, https://www.facebook.com/StopSopaNow (last visited Oct. 24, 2015).

149. Yvonne Juris, *Images from the "Justice for All March*," MSNBC (Dec. 22, 2014), http://www.msnbc.com/politicsnation/images-the-justice-all-march; Christopher Robbins, *Photos: Millions March Shuts Down Brooklyn Bridge, NYPD Says They Must "Draw the Line*," GOTHAMIST (Dec. 14, 2014), http://gothamist.com/2014/12/14/photos_protesters_shut_down_brookly.php.

150. Robert McMillan, *In Iran, Cyber-Activism Without the Middle-Man*, COMPUTERWORLD (Jun. 18, 2009), http://www.computerworld.com/article/2525624/government-it/in-iran-cyber-activism-without-the-middle-man.html.

Geneva-based haggling put together.'"[151] Others credited social media platforms like YouTube, Twitter, and Facebook for doing more for progressive Arab politics than either the UN or the European Union. Mark Pleife, former deputy national security advisor in the Bush White House, went so far as to campaign for Twitter's nomination for the Nobel Peace Prize, arguing that "without Twitter, the people of Iran would not have felt empowered and confident to stand up for freedom and democracy."[152] While skeptics maintain that "liking" a subversive post on Facebook, or "re-Tweeting" a development on Twitter in an activism movement is hardly capable of bringing about the so-called "Fourth Wave" of democratization in the Arab world,[153] and this may have a degree of truth, it cannot be disputed that social media platforms have the ability to, at the very least, raise people's awareness in a way that print journalism or other older forms of media cannot.[154]

Hence, social media platforms such as Twitter or Facebook may likewise be utilized to publicize the anti-CISPA discourse and to expose CISPA's potential to violate the privacy rights of outspoken citizens exercising the First Amendment right to free speech and assembly. Such a campaign would likely target a wide-reaching audience of Internet users to effectively make an impact on defeating harmful cybersecurity legislation.

V. Conclusion

In 1940, Attorney General Robert Jackson recognized that using broad labels like "national security" or "subversion" to invoke the vast power of the government is dangerous because there are "no definite standards to determine what constitutes a 'subversive activity,' such as for murder or larceny."[155] This author applauds our generation of concerned citizens for

151. *The Clinton Internet Doctrine*, WALL ST. J. (Jan. 23, 2010), http://www.wsj.com/articles/SB10001424052748704320104575014560882205670.

152. Golnaz Esfandiari, *The Twitter Devolution*, FOREIGN POL'Y (June 8, 2010), http://foreignpolicy.com/2010/06/08/the-twitter-devolution/.

153. Malcolm Gladwell, *Small Change: Why the Revolution Will Not Be Tweeted*, THE NEW YORKER (Oct. 4, 2010) (arguing that social media platforms merely enable Internet users to partake in an effort they deem to be meaningful, without making any real sacrifices; these non-meaningful clicking and typing efforts are therefore part in parcel of a "Slacktivist" rather than an activist movement).

154. *See* Sarah Joseph, *Social Media, Political Change, and Human Rights*, 35 B.C. INT'L & COMP. L. REV. 145, 186 (2012) ("Gladwell too readily ignores the value of social media in States that efficiently suppress information and conversation, and in developing States, where long-voiceless people are suddenly connected to each other and to the outside world" and that in the developed world, "the increase of unfiltered connections between people of different cultural, political, and economic outlooks is likely to have some unprecedented and beneficial consequences for the development of local, national, regional, and global activism.").

155. SENATE SELECT COMM., *supra* note 1.

standing up in the wake of widespread police brutality and structural racism to ensure that law and order is carried out in a just manner. But it would be wise to remember broadly-defined "subversive activity" has historically been closely monitored, and that democratic forms of resistance risk being compromised when government tactics operate outside the bounds of the Constitutional principles we hold in such high esteem.

This note has examined the U.S. history of surveillance of marginalized communities in times of increased subversion of government policies. By using the Bloody Sunday protest, and the increased surveillance of Black demonstrators through the FBI's development of COINTELPRO as an analytical framework, the paper suggests that demonstrators involved in the Black Lives Matter campaign should be especially concerned with legislation regarding government surveillance. For that reason, this note argues that civil rights protestors, particularly those belonging to racial and ethnic minority groups, should unite against legislation such as CISPA. CISPA's stated intent is to help gather and facilitate the sharing of personal information between the public and private technology sectors, which arguably implicates the surveillance doctrine of the Fourth Amendment, and requires that the government obtain a warrant.[156] This note examines the incredibly successful Stop SOPA campaign of 2012 and encourages future cybersecurity demonstrators to adopt a similar discursively powerful strategy and to deploy that strategy online in order to stop the Legislature from passing CISPA for good.

Moreover, if public interest considerations are to be included in future cybersecurity legislation, the public will need to advocate for itself, rather than relying on self-interested technology companies, which will be happy to pass such legislation, given the government's grant of immunity. The tech industry and the public's interests may have serendipitously converged for stopping SOPA and PIPA, but this is not the norm. Therefore, this note encourages Internet users and activists across the nation to stay informed of surveillance legislation in order to ensure that their fundamental rights are adequately protected.

156. The Supreme Court has held that the "Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures." Katz v. United States, 389 U.S. 347, 353 (1967). Moreover, the government's surveillance of U.S. citizens constitutes a "search and seizure" within the meaning of the Fourth Amendment where that surveillance "violate[s] the privacy upon which [an individual] justifiably relied." *Id.**

* * *